UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JAMES ROWE, on behalf of himself and all others similarly situated, Plaintiff, v. UNICARE LIFE AND HEALTH INSURANCE COMPANY, and WELLPOINT, INC., both Indiana Corporations, Defendants.	Case No. 09 CV 2286 Judge William J. Hibbler

DEFENDANTS' MEMORANDUM OF LAW
IN SUPPORT OF THEIR MOTION TO DISMISS

I. PRELIMINARY STATEMENT

Unicare Life and Health Insurance Company ("Unicare") and Wellpoint, Inc. ("Wellpoint") move under Federal Rules of Civil Procedure ("Rules") 8(a)(2) and 12(b)(6) to dismiss the Complaint of Plaintiff James Rowe.

Plaintiff, based on his own factual allegations, has not been harmed in any way, shape, or form. At most, Plaintiff alleges that Defendants temporarily made his member identification number (which may include his Social Security number) and certain pharmacy/medical data about him "accessible to the public via the Internet." (Complaint ¶ 9.) Plaintiff does not allege that any third party actually looked at his records while they were "accessible".

Plaintiff certainly does not allege that he is the victim of actual or attempted identity theft as a result of information about him being "made available". Plaintiff does not allege any actual result – at all – of his information being "made available".

In *lieu* of factual allegations about actual or imminent harm, Plaintiff presents only speculation. Plaintiff's Complaint implies that if information about Plaintiff were available on the Internet, *maybe* someone viewed that information, and *maybe* that reader has ill intent, and *maybe*, as a consequence, harm will someday, somehow, befall Plaintiff. Even if genuine, Plaintiff's worry about future hypothetical harm does not satisfy the pleading standard required

to bring a case against these Defendants here and now. Courts in the Seventh Circuit and across the country, faced with such compound chains of conjecture, have granted motions to dismiss, and this case should, for the reasons addressed in more detail below, meet that end.

There *is* a federal statute which governs the protection of health information. That is the Health Insurance Portability and Accountability Act ("HIPAA"). But Plaintiff, himself a class action attorney, knows that HIPAA provides no private right of action.[1] By design, HIPAA relies solely on government enforcement. Plaintiff, undeterred, tries here to shoehorn his grievance into a series of other, inapposite causes of action.

Plaintiff first tries the Fair Credit Reporting Act ("FCRA"). But the FCRA imposes liability only when the Defendant has communicated consumer information. And Plaintiff does not allege that Defendants communicated his information to anyone, anywhere, only that his information was temporarily "made available". That something is "made available" online does not mean anyone has read it.

Plaintiff also tries to couch his claims under the Illinois Insurance Information and Privacy Protection Act. But that Act punishes only wrongful disclosures, and compensates for only actual damages. Plaintiff does not allege that Defendants disclosed anything to anyone, much less that there was any resulting damage.

Lastly, Plaintiff suggests that this Court should entertain his claim for potential future injury under Illinois common law for negligence, breach of implied contract, and breach of privacy. Again, Plaintiff's claims are hamstrung by the lack of actual present damage. Plaintiff can only say he feels "anxiety" and "emotional distress". Illinois common law does not permit such claims even for persons who have been potentially exposed to deadly diseases like HIV.

Moreover, the Illinois legislature has legislated on data security breaches. The resulting law requires the database owner to disclose the breach, nothing more. The law does not require

[1] *See, e.g., Butler v. Ill. Dept. of Transp.*, 533 F. Supp. 2d 821, 827 (N.D. Ill. 2008)("HIPAA does not imply a private right of action"), *Levin v. Board of Educ. of City of Chicago*, 470 F. Supp. 2d 835, 838 (N.D.Ill. 2007) ("the court dismissed the HIPAA claims because there is no private right of action for HIPAA violations"); *Doe v. Bd. of Trs. of Univ. of Ill.*, 429 F. Supp. 2d 930, 944 (N.D.Ill. 2006) ("Every court to have considered the issue, however, has concluded that HIPAA does not authorize a private right of action. The Court agrees with these decisions; HIPAA provides civil and criminal penalties for improper disclosures of medical information, but it does not create a private cause of action, leaving enforcement to the Department of Health and Human Services alone") (internal citations omitted).

any compensation be paid to anyone following a breach. This Court should follow the recent advice and example of the Seventh Circuit – in this very context – and refuse to create a state law remedy where the state legislature has declined to do so.

Plaintiff volunteers to manufacture his own harm, if it will keep him in court, by pro-actively purchasing credit monitoring beyond that which was provided by Unicare. But of course, a plaintiff cannot create a cognizable case from thin air by means of self-inflicted "injury".

In short, Plaintiff is a man speculating that something may have happened which someday may cause him harm. Here and now, Plaintiff's Complaint should be dismissed.

II. FACTUAL ALLEGATIONS

Solely for purposes of this Motion to Dismiss, we will assume that all of Plaintiff's factual allegations are true. Plaintiff alleges that between 2003 and 2005, he was a customer of Unicare. (Complaint ¶ 8.) Plaintiff further alleges that "in the regular course of their business," Defendants "obtain and possess a consumer's Private Health Information, such as their name, social security number, incomes, employment information, phone number, medical history, prescription records, medical diagnoses, medical treatment history, etc." (Complaint ¶ 7.) Defendants "collect," "use," and "retain" such information, and make it "available to [their] employees, affiliates, or others who need to service or maintain [a] policy, to conduct insurance transactions and functions, or for other legally permitted or required purposes." (*Id.* ¶¶ 28-29.)

Plaintiff then incorporates by reference two letters, Exhibits A and B to the Complaint. Exhibit A is an April 2, 2008 letter from counsel for Unicare to the New Hampshire Attorney General. That letter noted, in part:

> Approximately one year ago [April 2007], it was discovered that a computer server that contained protected health information (PHI) was not properly secured by a third party vendor for a period of time, which caused the PHI of some members to be temporarily accessible via the internet. The PHI contained member ID numbers (which, in some cases, included a social security number) and certain pharmacy/medical data that pertained to the member or the member's dependents enrolled under the member's health plan.
>
> (Complaint at Ex. A.)

The letter goes on to note that Unicare "notified the members who we determined might have been impacted. On December 27, 2007, we determined that the PHI of additional members

may have been accessible via the internet at the time of this incident… a letter regarding this incident will be mailed to all affected members." (*Id*.)

Exhibit B to the Complaint is an April 11, 2008 letter to Plaintiff, informing him of the same incident, and that "this PHI included information that pertained to you and/or your dependants enrolled under your health plan." In the letter, Unicare further offered Plaintiff one year of credit monitoring free of charge "to further reduce any potential risk to you or your family members." (Complaint at Ex. B.)

These letters form the entire basis of Plaintiff's factual allegations.

III. LEGAL STANDARD

Twombly controls the disposition of this current Motion. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007). In *Twombly*, the United States Supreme Court re-emphasized "the threshold requirement of Rule 8(a)(2) that the 'plain statement' possess enough heft to 'sho[w] that the pleader is entitled to relief.'" *Id*. at 557.

To survive a Rule 12(b)(6) motion, the Court held that a Complaint's factual allegations "must be enough to raise the right to relief above the speculative level." *Twombly*, 550 U.S. at 555. "[S]omething beyond the mere possibility of loss causation must be alleged, lest a plaintiff with a largely groundless claim be allowed to take up the time of a number of other people, with the right to do so representing an *in terrorem* increment of the settlement value." *Twombly* at 557-588 (citation omitted).

The Seventh Circuit has embraced *Twombly* wholeheartedly. *See, e.g., Limestone Dev. Corp. v. Vill. of Lemont, Ill.*, 520 F.3d 797, 802-804 (7th Cir. 2008) (affirming dismissal of a "threadbare" Complaint). "*Bell Atlantic Corp. v. Twombly* teaches that a defendant should not be forced to undergo costly discovery unless the complaint contains enough detail, factual or argumentative, to indicate that the plaintiff has a substantial case." *Id*. at 802-03 (citations omitted).

IV. LEGAL ARGUMENT

A. Plaintiff States No Claim Under the Fair Credit Reporting Act

Plaintiff alleges that Defendants violated the Fair Credit Reporting Act ("FCRA"). Plaintiff alleges that, by temporarily making information about him available on the Internet, Defendants engaged in improper dissemination. Plaintiff further alleges that Defendants failed

to maintain reasonable procedures to prevent improper dissemination. These claims have no merit.

The FCRA is not concerned with just any consumer information. The FCRA is concerned with the protection of "consumer reports." The term "consumer reports" is defined by 15 U.S.C.A. §1681a(d)(1). Per that section:

> The term "consumer report" means any written, oral, or other **communication** of any information by a consumer reporting agency **bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living** which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for-- (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title.
>
> (Emphasis added.)

If this case were to continue into discovery, Defendants would demonstrate that they are not consumer reporting agencies. However, even at this Motion to Dismiss stage, two independently fatal flaws in Plaintiff's FCRA claims exist. Plaintiff does not plead any communication of information. And the data "made available" did not bear on any of the FCRA's enumerated factors. For both these reasons, Plaintiff's FCRA claims should be dismissed.

1. Plaintiff Fails to Plead That a Communication Took Place

Plaintiff claims, over and over, that his records or those of the alleged class were temporarily "accessible to the public via the Internet," "made available to the public," "made available and accessible." (*See, e.g.*, Complaint ¶¶ 9, 11, 12, 14.) Plaintiff studiously avoids any allegation that his records were actually accessed by anyone. Nothing in the facts alleged, and nothing in the letters attached to the Complaint, suggests that any third party actually viewed Plaintiff's records during the period of alleged availability.

In short, Plaintiff does not plead a "communication". A "communication," as defined by *Black's Law Dictionary* 296 (8th edition 2004), is "[t]he expression or exchange of information by speech, writing, gestures, or conduct; the process of bringing an idea to another's perception". *Accord, Webster's Third New International Dictionary* 460 (1961) ("the act or action of imparting or transmitting"). As every child with a string and two tin cans knows, there is no communication if no one is on the other end.

The decision in *Harrington v. Choicepoint, Inc*., 2:05-cv-1294-MRP-JWJ (C.D. Cal. Oct. 11, 2006) (attached hereto as Exhibit A) is instructive. In *Harrington*, as here, plaintiffs argued that because their information was made available to third parties, it had been communicated to those third parties for FCRA purposes. The *Harrington* court flatly rejected that argument. The Court held plaintiffs did not have a FCRA claim because the third party had not accessed the plaintiffs' information and thus there was no "communication." *Id.* at 9-11. "The plain meaning of that word ["communication"] . . . at a minimum requires some act of transmission of information from one source to another." *Id.* at 10. In other words, without someone accessing the information, there was no "communication."

If then Plaintiff cannot plead here, consistent with the standards of Rule 11, that someone actually viewed his records, then Plaintiff has no case under the FCRA. Without "written, oral, or other communication," by definition there is no "credit report," "*i.e*., there cannot be a consumer report without disclosure to a third party." *Wantz v. Experian Info. Solutions*, 386 F.3d 829, 833-34 (7th Cir. 2004), *abrogated on other grounds by Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47 (2007). If there is no communication, there is no consumer report, and no claim can stand that the non-existent consumer report was issued without a proper purpose.

Apparently cognizant that he has pled no facts surrounding any third party viewing his records, Plaintiff also attempts to couch his FCRA claim as a violation of 15 U.S.C.A. §1681e(a). That section of the FCRA requires "reasonable procedures designed to limit the furnishing of Consumer Reports to the permissible purposes outline[d] under FCRA." (Complaint ¶ 31.) Unfortunately for Plaintiff, courts have construed §1681e(a) as also requiring improper disclosure before suit can be brought. *See, e.g., Wantz*, 386 F.3d at 833-34 (dismissing a "reasonable procedures" claim where no improper disclosure had been made); *Washington v. CSC Credit Servs. Inc.*, 199 F.3d 263, 267 (5th Cir. 2000) ("we find that the actionable harm the FCRA envisions" in requiring reasonable procedures "is improper disclosure, not the mere risk of improper disclosure").

In *Wantz*, the Court construed §1681e(b), which requires "reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates." 386 F.3d at 832. The Court held that where there is no evidence that information was disclosed to any third party, there was no "consumer report" and plaintiff's suit alleging lack of "reasonable procedures" must be dismissed. *Id*. at 833-34. "Without such a report, there

could be no duty to follow reasonable procedures regarding the report, nor could damages flow from a breach of that duty." *Id*. at 834.

In the case at bar, Plaintiff has not alleged that information about him was actually communicated to anyone. Plaintiff may speculate that someone *may* have examined his records while they were temporarily available on the Internet. Such speculation does not satisfy *Twombly*. Plaintiff's failure to allege a "communication" of *his* records to any third party is independently fatal to his claims under the FCRA.

2. The Information Made Available Does Not Bear On Any Of The Enumerated Factors

Plaintiff alleges that Defendants wrongly made available a consumer report containing information on Plaintiff. As noted above, even if Plaintiff were right that information about him was made available, it did not constitute a "communication" (since Plaintiff alleges nobody to whom it was communicated). There is an independently sufficient reason to dismiss Plaintiff's FCRA claims. Contrary to the very definition of a "consumer report," the information in question did not "bear[] on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living." 15 U.S.C.A. §1681a(d)(1).

As shown in the letters Plaintiff attached to his Complaint and relies upon, the information temporarily made available on the Internet included "member ID numbers (which, in some cases, included a social security number) and certain pharmacy/medical data that pertained to the member or the member's dependents enrolled under the member's health plan." (Complaint at Ex. A.) Courts have found that this type of information does not bear on the enumerated factors and does not constitute a consumer report for FCRA purposes.

Consider, for example, *In re Northwest Airlines Privacy Litig.*, Case No. Civ.04-126, 2004 WL 1278459 (D.Minn. June 6, 2004) (dismissing FCRA claims on a Rule 12(b)(6) motion). In that case, the defendant airline had provided passenger information to the government. This included every passenger's "name, flight number, credit card data, hotel reservation, car rental, and any traveling companions." *Id.*, at *1. Plaintiffs sued under the FCRA. The Court found that the plaintiff's FCRA claims "fail as a matter of law" because "[t]his limited information cannot fairly be said to be information "bearing on a consumer's credit worthiness, credit standing, [or] credit capacity." *Id.* at *3. By the same token, Plaintiff's name and pharmacy information do not bear on the enumerated factors.

In *Harrington v. Choicepoint*, plaintiffs alleged that the defendant consumer reporting agency had sold information about plaintiffs to third persons with criminal intent. (Ex. A.) Plaintiffs brought an FCRA action. The Court found that the FCRA did not apply because the only information at issue was name, address, telephone number, date of birth, Social Security number, and driver's license number. *Harrington*, slip op. 11-13 (Ex. A). This "very basic demographic and identity related information" would not be useful to a potential creditor and hence does not "meet the content standard for a consumer report envisioned by Congress when it drafted the seven-factor test." *Id*. at 12-13.

Likewise, Plaintiff's Social Security Number (even if included in his member identification number) and pharmacy/medical data do not bear on the enumerated factors. The information at question did not constitute a credit report. For this independently-sufficient reason, Plaintiff has not stated a viable FCRA claim.

B. Plaintiff States No Claim Under the Insurance Information and Privacy Protection Act

Plaintiff claims that by making information about him available on the Internet, Defendants violated the Insurance Information and Privacy Protection Act. 215 ILCS 5/1001 *et seq*. That Act provides that, "An insurance institution, agent or insurance-support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction," with certain exceptions not applicable here. *Id.* at § 5/1014. Again, Plaintiff fails to state a claim. He does not allege that his information was actually disclosed to any third party. He only pleads that his information was "available" to such third parties, should they have chosen to search it out.

Moreover, the Act provides that "no individual shall be entitled to a monetary award which exceeds the *actual damages* sustained by the individual as a result of a violation of Section 1014 of this Article." 215 ILCS 5/1021(B) (emphasis added). But Plaintiff presents no actual damages, only hypothetical ones.

If Plaintiff had been the victim of identity theft, he presumably could point to his unreimbursed out-of-pocket losses as "actual damage". The term "actual damages" has been construed to mean compensatory damages, to the exclusion of exemplary or punitive damages. *See, e.g., White v. Prenzler*, 19 Ill. App. 2d 231, 238, 153 N.E.2d 477, 481 (3d Dist. 1958). But Plaintiff alleges no injury for which Illinois law would provide compensation.

Plaintiff alleges "anxiety [and] emotional distress," but says nothing in support of these claims. (Complaint ¶ 67.) Under Illinois law, "[e]motional distress constitutes legally cognizable damage only where the distress is particularly severe. The law intervenes only where the distress inflicted is so severe that no reasonable man could be expected to endure it." *Doe v. Northwestern Univ.*, 289 Ill. App. 3d 39, 45, 682 N.E.2d 145, 150 (1st Dist. 1997) (internal quotation omitted). In *Doe*, plaintiff sought recovery because a dental student who participated in his treatment had later been diagnosed with HIV. The trial court denied recovery, and the Appellate Division affirmed.

> Defendants' letter itself shows that plaintiffs had reason to fear that they might have been infected with HIV. However, not all reasonable fears of AIDS are compensable. Plaintiffs have not alleged facts that could support a finding that they faced more than an extremely remote possibility of contracting AIDS. In the absence of a particularly substantial risk of HIV infection, plaintiffs' reasonable fears were not severe enough to warrant tort compensation. Plaintiffs have not suffered legally cognizable damages.
>
> *Id*. at 50-51, 682 N.E. 2d at 153.

Likewise, the potential exposure of Plaintiff's information to a third party is not sufficient to support a claim for emotional damages or anxiety. Identity theft is serious, but not more serious than HIV and AIDS. Plaintiff has not alleged facts that could support a finding that he faces more than an extremely remote possibility of harm. Under *Doe* and *Twombly*, Plaintiff's Insurance Information and Privacy Protection Act claim must be dismissed for failure to plead cognizable damages.

It is immaterial that Plaintiff claims he must now purchase credit monitoring. *See, e.g., Aliano v. Tex. Roadhouse Holdings LLC*, Case No. 07 C 4108, 2008 WL 5397510 (N.D.Ill. Dec. 23, 2008). In *Aliano*, plaintiff claimed the merchant included more information on the electronically printed credit or debit card receipts provided to its customers than is permitted by the Fair and Accurate Credit Transaction Act ("FACTA"). *Id.* at *1. Plaintiff, therefore, alleged that he was compelled to purchase credit monitoring. *Id.* After a survey of privacy caselaw, the Court found that such a purchase did not constitute a compensable injury. *Id. at *2;* a*ccord, Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007) (dismissing a suit premised on "Plaintiffs' allegation that they have incurred or will incur costs in an attempt to protect themselves against their alleged increased risk of identity theft"); *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1020-21 (D. Minn. 2006) (rejecting plaintiff's negligence

claims, finding that the plaintiffs' "expenditure of time and money" in "monitoring their credit" does not constitute injury or damages because it "was not the result of any present injury, but rather the anticipation of future injury that has not materialized"); *Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F. Supp. 2d 775, 779-80 (W.D. Mich. 2006) (holding plaintiff was not entitled to credit monitoring under Michigan law, not even to secure her "peace of mind").

"Aliano does not allege that he has been actually harmed by Defendants' actions. Instead, Aliano alleges only that he has purchased credit monitoring services in order to guard against harms that may or may not occur in the future." *Aliano,* 2008 WL 5397510, at *4. Therefore, the Court dismissed Aliano's claim for failure to state a cause of action upon which relief could be granted.

C. Plaintiff States No Claim Under Common Law

Plaintiff lists claims for negligence, breach of implied contract, and for invasion of privacy. These claims, too, fail because Plaintiff has not alleged that anything happened. Plaintiff has not alleged damages, as he must to state a claim for negligence. *See, e.g., Shehade v. Gerson*, 148 Ill. App. 3d 1026, 1031, 500 N.E.2d 510, 514 (1st Dist. 1986) ("Where the damages in a negligence action are based on conjecture or speculation, the action must be dismissed for recoverable damages are an essential element of every negligence action").

Plaintiff has not alleged any benefit which Defendants obtained by "making available" information about him, nor any detriment he suffered. Each deficiency is independently-sufficient to preclude a claim for breach of implied contract. *See, e.g., Suarez v. Pierard*, 278 Ill. App. 3d 767, 773, 663 N.E.2d 1039, 1044 (3rd Dist. 1996) (holding that an implied contract "is equitable in nature, predicated on the fundamental principle that no one should unjustly enrich himself at another's expense").

Plaintiff has not alleged a single person to whom his information was published. *See, e.g., Wynne v. Loyola Univ. of Chicago*, 318 Ill. App .3d 443, 453, 741 N.E.2d 669, 676-77 (1st Dist. 2000) (noting "publicity" is an element of the tort for public disclosure of private facts, and that publicity is defined as "communicating the matter to the public at large or to so many persons that the matter must be regarded as one of general knowledge").

And, even if Plaintiff were to suddenly allege that his information was viewed, he still has failed to allege that the viewing had any detrimental result. Illinois law does not recognize a cause of action for the creation of inchoate risks which never came to fruition. The Illinois

Supreme Court has determined that an otherwise uninjured plaintiff cannot proceed to sue based solely on allegedly increased risk of future injury. *Williams v. Manchester*, 228 Ill. 2d 404, 425, 888 N.E.2d 1, 13 (2008) ("as a matter of law, an increased risk of future harm is an element of damages that can be recovered for a present injury--it is not the injury itself").

This Court should decline to engraft onto the substantive law of Illinois a cause of action for which injury is not required. *Cf. Pisciotta v. Old Na'l. Bancorp*, 499 F.3d 629, 638-40 (7th Cir. 2007) (dismissing putative class action arising from data security suit for lack of compensable injury). In *Pisciotta*, the Court had to decide whether Indiana law would permit a suit based on "increased risk" following a data security breach. The Court looked at Indiana's statute on data security breach notification. Importantly, the Court found that, "The provisions of the statute applicable to private entities storing personal information require only that a database owner disclose a security breach to potentially affected consumers; they do not require the database owner to take any other affirmative act in the wake of a breach" and that the law "imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow." *Id*. at 637.

> Had the Indiana legislature intended that a cause of action should be available against a database owner for failing to protect adequately personal information, we believe that it would have made some more definite statement of that intent. Moreover, given the novelty of the legal questions posed by information exposure and theft, it is unlikely that the legislature intended to sanction the development of common law tort remedies that would apply to the same factual circumstances addressed by the statute.
>
> *Id*. at 638.

An examination of Illinois's Personal Information Protection Act, 815 ILCS 530/1, *et seq*., compels the same result. As with the Indiana statute, the Illinois law requires only disclosure of breaches. The statute provides a private right of action to an Illinois citizen only for the failure to disclose. The Illinois law "imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow." *Pisciotta*, 499 F.3d at 637. Given that background, as the Seventh Circuit found with respect to Indiana, "it is unlikely that the [Illinois] legislature intended to sanction the development of common law tort remedies that would apply to the same factual circumstances[.]" *Id*.

Another Court, presiding over multiple class actions pursuant to an MDL transfer, dismissed consumer claims based on "increased risk of identity theft". In *Hannaford*, plaintiffs

were supermarket customers. *In re Hannaford Bros. Co. Customer Data Security Breach Litig.*, MDL Case No. 2:08-MD-1954, 2009 WL 1316178, *1 (D. Me. May 12, 2009). These plaintiffs alleged that:

> third-party wrongdoers obtained access to [Hannaford's] information technology systems and, until containment of this security breach …stole private and confidential debit card and credit card information, including up to an estimated 4.2 million debit card and credit card numbers, expiration dates, security codes, PIN numbers and other information belonging to [the] [p]laintiffs and other customers ... who had used debit cards and credit cards to transact purchases at supermarkets owned or operated by [Hannaford].

Id. (internal quotations omitted).

Some *Hannaford* plaintiffs alleged to be actual identity theft victims. *Id*. "The plaintiffs have sued Hannaford for damages for those losses and for injunctive relief. In addition to damages, they want me to order Hannaford to provide credit monitoring to all affected customers and notify each of them 'exactly what private and confidential financial and personal information of each Class member was exposed to theft and was, in fact, stolen.'" *Id*. at *3.

The plaintiffs brought multiple putative consumer class actions. The defendant moved for dismissal under Rule 12(b)(6). The *Hannaford* court granted that motion except as to consumers who had suffered actual, unreimbursed, out-of-pocket loss due to actual identity theft or unauthorized account takeover.

The *Hannaford* court found, as to "[c]onsumer plaintiffs who never had fraudulent items posted to their accounts," that these plaintiffs had not plead a cause of action upon which relief could be had. *Id*. at *13. Both Maine's unfair trade practices act and Maine's common law predicated recovery on proof of injury. Emotional distress damages were not available, except under limited circumstances not at issue in *Hannaford* (and not alleged in this case). Because these consumer plaintiffs alleged no cognizable injury, as to them, the court granted defendant's Rule 12(b)(6) motion.[2]

[2] In addition to the cases cited above, the authorities for Rule 12(b)(6) dismissal of claims of "increased risk of identity theft" are abundant. *See, e.g., Cherny v. Emigrant Bank*, Case No. 08 Civ 5359, 2009 WL 690248 (S.D.N.Y. March 12, 2009) (dismissing data security class action for lack of injury under New York law); *Pinero v. Jackson Hewitt Tax Serv., Inc*., Case No. 08-3535, 2009 WL 43098 (E.D.La. Jan. 7, 2009) (same, under Louisiana law); *Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc*., Case No. 08-1568, 2009 WL 799760 (E.D.La. Mar. 24, 2009) (same); *Melancon v. La. Office of Student Fin.Assistance*, 567 F.Supp.2d 873 (E.D.La. 2008) (same); *Shafran v. Harley-Davidson, Inc*., Case No. 07

Dismissal of "increased risk of identity theft" suits has become a sufficiently obvious result that one federal court this year, *sua sponte*, dismissed a *pro se* Complaint arising from a data security breach. *Hinton v. Heartland Payment Sys., Inc*., Case No. 09-594 (MLC), 2009 WL 704139 (D.N.J. March 16, 2009). This Complaint alleged that plaintiff's credit card information had been stolen from defendant, a credit processing company. The Complaint further alleged that the theft had put plaintiff at "increased risk of fraud and identity theft." *Id*. at *1. "[I]t appearing that Hinton's allegations of injuries amount to nothing more than mere speculation," the Court dismissed his case for being "frivolous and for failure to state a claim". *Id.*

V. CONCLUSION

Plaintiff's Complaint should be dismissed in its entirety. Taking all of the facts alleged as true, Plaintiff does not raise his right to recovery beyond the level of mere speculation.

Dated: May 22, 2009

Respectfully submitted,

UNICARE LIFE AND HEALTH INSURANCE COMPANY, and WELLPOINT, INC., *Defendants*

By: /s/ Marina C. Santini
One of their attorneys

Mark S. Melodia (admitted *pro hac vice*)
Paul Bond (admitted *pro hac vice*)
REED SMITH LLP
Princeton Forrestal Village
136 Main Street, Suite 250
Princeton, N.J. 08540
(609) 987-0050

David Z. Smith (ARDC # 6256687)
Marina C. Santini (ARDC # 6290668)
REED SMITH LLP
10 South Wacker Drive
Chicago, IL 60606-7507
(312) 207 1000
(312) 207 6400 (fax)

Civ. 01365, 2008 WL 763177 (S.D.N.Y. Mar. 20, 2008) (dismissing all claims from data security breach); *Ponder v. Pfizer, Inc*., 522 F.Supp.2d 793, 798 (M.D.La. 2007) (dismissing claim for credit monitoring under Louisiana law, holding that "injury accrues when the compromised data are actually used by a third party to steal someone's identity").

CERTIFICATE OF SERVICE

I hereby certify that on May 22, 2009, I electronically filed the foregoing **DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION TO DISMISS** with the Clerk of the Court using the CM/ECF system which sent notification of such filing to the following:

BARNOW AND ASSOCIATES, P.C.
Ben Barnow
Sharon Harris
Erich Schork
Blake Strautins
One North LaSalle Street, Suite 4600
Chicago, IL 60602
(312) 621-2000
Attorneys for Plaintiff

LARRY D. DRURY, LTD.
Larry D. Drury
205 West Randolph, Suite 1430
Chicago, IL 60606
(312) 346-7950
Attorneys for Plaintiff

/s/ Marina C. Santini
REED SMITH LLP
10 South Wacker Drive
Chicago, IL 60606-7507
(312) 207 1000
(312) 207 6400 (fax)

Attorneys for Defendants

US_ACTIVE-101644871.5